13

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/783,146	02/13/2001	Marc D. VanHeyningen	05313.00003	1516

7590 12/20/2005

Banner & Witcoff, Ltd.
1001 G. Street, N.W.
Washington, DC 20001-4597

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 12/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/783,146	**Applicant(s)** VANHEYNINGEN ET AL.	
	Examiner Kambiz Zand	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/26/2005 and interview on 11/09/05*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-20,22-27,29,31-43,45 and 47-58* is/are rejected.

7)☒ Claim(s) *8,21,28,30,44 and 46* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 June 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *10/11/05*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1-58 are pending.

Response to Arguments

4. Applicant's arguments with respect to the claims filed on 10/26/2005 and on the interview conducted on 11/09/2005 have been fully considered but they are not persuasive.

- As per applicant's arguments traversing the double patenting rejection rendered in the previous office action, Examiner makes the following remarks:

- Claim 1 of the application 09/782,593 discloses transmission of records between two computers where the records are encrypted by one computer and decrypted by the receiving computer. Such elements also present in the claim 1 of the instant application. The addition of the third computer and transmission of session information to it by the second computer does not change the fact that the process of passing the information for encryption and decryption is repeated process that it is taken place between the first two computers and such a addition is only a design choice for intended use. The preamble of the claims involve refers to computer network, therefore it would have been obvious to one of ordinary skilled in the art at the time the invention was made to transmit the session information from one computer to another (example, from second to the third; or first to the second or vice versa or to other terminals in the system network) in order to enable the receiving terminal capabilities for decryption of the encrypted records receive or vice versa. Such motivation is obvious since without transfer of such session information the received terminal in unable to perform decryption of the encrypted records received. The double patenting rejection rendered are based on such obviousness since all other limitations of the claims are anticipated by the application number 09/782, 593, making such above difference with the instant application as obvious. As far as claim 38 is concerns, the third computer has a cache memory, however such process is again obvious as disclosed above. The storage design choice is also obvious since a terminal can store such session information in a memory, hard disk, cache memory, external storage, removable storage, etc, but again it does not change the fact that the process between the first computer and the second computer with respect to encrypting the record, transmission of it and decryption of it is being repeated now between the second and the third computer as discussed above where the third computer has an storage element, something inherent in the first and the second computer. Examiner also refers Applicant to A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). Therefore the applicant's arguments with respect to the double patenting rejection are not persuasive.

- In response to applicant's argument that the references fail to show the third computer and the transfer of the session information between the second and the third computer, examiner makes the following remarks:

- Fig.1 disclose a network with many computers, terminal a through terminal N. therefore the third computer is present in the embodiment of the invention.

- Col.5, lines 7-27 disclose that each terminal has the capabilities for encryption and decryption and the information are transmitted through the communication channel between the terminals. Lines 34-42 also disclose that such transmitted information may include user's secret or split-key. Therefore information on which a terminal can encrypt or decrypt is being transmitted between the terminals (Terminal A through terminal N which corresponds to applicant's computer 1 through computer N=3).

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

   A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

   Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. **Claims 1, 20, 38 and 47** provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 10, 16 and 23 of copending Application No. 09/782,593. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following reasons:

- Claim **1** of instant application is obvious since it does not recite "by incorporating a nonce", "by using the nonce in combination with a previously shared encryption key to decrypt each of the data records", as recited in claim 1 of copending Application No. 09/782,593; further more the claim 1 of the instant application has an added limitation "in the second computer, transmitting session information for encrypting and decrypting data records to a third computer". However it would have been obvious to one of ordinary skilled in the art to transmit session information to another computer for the purpose of backup or secure transmission of data records.

- Claim **20** of instant application is obvious over claim 10 of copending Application No. 09/782,593; the claim 20 of the instant application has an added limitation " in the proxy server, transmitting session information including the previously shared encryption key for use in decrypting the plurality of data records to another server". However it would have been obvious to one of ordinary skilled in the art to transmit session information to another computer for the purpose of backup or secure transmission of data records.

- Claim **38** of instant application is obvious over claim 16 of copending Application No. 09/782,593; the claim 38 of the instant application has an added limitation " a third computer coupled to the second computer and having a cache memory for storing at least the encryption key". However it would have been obvious to one of ordinary skilled in the art to transmit security information to another computer for the purpose of backup or secure transmission of data records.

- Claim **47** of instant application is obvious since it does not recite "by incorporating a nonce", "by incorporating the nonce encrypted such that the remote computer can decrypt each data records by using the nonce in combination with a previously shared encryption key", as recited in claim 23 of copending Application No. 09/782,593; "a first computer" in the instant application corresponds to co-pending application's "remote computer" further more the claim 47 of the instant application has an added limitation "transmitting session information for decrypting the encrypted data records to a second computer". However it would have been obvious to one of ordinary skilled in the art to transmit session information to another computer for the purpose of backup or secure transmission of data records.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

7. **Claims 1-4, 10, 11, 12, 15, 16, 20, 24, 25, 27, 29, 34, 38, 39, 43, 45, 47, 48, 54, 56 and 57** are rejected under 35 U.S.C. 102(e) as being anticipated by Fisher (6,216,229 B1).

As per claims 1 and 47 Fisher (6,216,229 B1) teach a method and a system of transmitting data securely over a computer network (see abstract; fig.6), comprising the steps of: (1) establishing a communication path between a first computer and a second computer (see fig.6, blocks 2010 and 2020); (2) encrypting and transmitting data records between the first computer and the second computer using an unreliable communication protocol, wherein each data record is encrypted without reference to a previously transmitted data record (see fig.6, block 2010); (3) in the second computer, receiving and decrypting the data records transmitted in step (2) without reference to a previously received data record (see fig.6, block 2020 and 2030; 2040); and (4) in the second computer, transmitting session information for encrypting and decrypting the data records to a third computer (see fig.1 where escrow agent represent the third computer that receives session information or shared secret). Also see col.4, lines 42-67; col.5-11 and col.12, lines 1-39.

As per claims 2 and 48 Fisher (6,216,229 B1) teach the method of claim 1, further comprising the step of, prior to step (1), establishing a reliable communication path between the first computer and the second computer and exchanging security credentials over the reliable communication path (see fig.4-6).

As per claim 3 Fisher (6,216,229 B1) teach the method of claim 2, wherein the step of exchanging security credentials comprises the step of exchanging an encryption key that is used to encrypt the data records in step (2) (see fig.4-6).

As per claim 4 Fisher (6,216,229 B1) teach the method of claim 2, wherein the session information includes at least a portion of the security credentials (see fig.4-6).

As per claims 10, 43 and 54 Fisher (6,216,229 B1) teach the method of claims 1 and

38, wherein step (2) is performed by a proxy server that encrypts data records received from another server (see fig.1-6).

As per claims 11, 12 Fisher (6,216,229 B1) teach a system with number of terminals (see fig.1) and all limitations of the method of claim 1 including establishes a communication path with the first computer; and encrypts and transmits data records to the first computer using an unreliable communication protocol, wherein each data record is encrypted without reference to a previously transmitted data record and by employing the session information above. Col.4, lines 42-48 establish a communication path between all computers (terminal a-n of fig.1 that corresponds to computer 1, 2, 3,4 ...,n).

As per claims 15 and 56 Fisher (6,216,229 B1) teach the method of claim 1, wherein the session information includes an encryption key that is used to encrypt data records in step (2) (see fig.4-6).

As per claims 16 and 57 Fisher (6,216,229 B1) teach the method of claim 1, wherein the session information is stored by the third computer in a cache memory using a hash function (see fig.1 and 6; col.4, lines 43-67 and col.5, lines 1-7).

As per claims 20 and 27 Fisher (6,216,229 B1) teach a method of securely transmitting a plurality of data records between a client computer and a proxy server using an unreliable communication protocol, comprising the steps of: (1) establishing a reliable connection between the client computer and the proxy server; (2) exchanging encryption credentials between the client computer and the proxy server over the reliable connection; (3) generating a nonce for each of a plurality of data records, wherein each nonce comprises an initialization vector necessary to decrypt a corresponding one of the plurality of data records; (4) using the nonce to encrypt each of the plurality of data records and appending the nonce to each of the plurality of data records; (5) transmitting the plurality of data records encrypted in step (4) from the client computer to the proxy server using an unreliable communication protocol; (7) in the proxy server, decrypting each of the plurality of encrypted data records using a corresponding nonce extracted from each data record and a previously shared encryption key; and (8) in the proxy server, transmitting session information including the previously shared encryption key for use in decrypting the plurality of data records to another server (as applied to claim 1 above and where examiner considers any terminal to be a client computer or a server).

As per claim 25 Fisher (6,216,229 B1) teach the method of claim 20, wherein step (6) is performed using an encryption key previously shared using a reliable communication protocol (see fig.1-6).

As per claim 33 Fisher (6,216,229 B1) teach the method of claim 20, wherein the session information includes authentication information for a user of the client computer (see fig.6).

As per claims 29 and 34 Fisher (6,216,229 B1) teach the method of claim 20, wherein the session information is stored by the other server in a cache memory using a hash function (see fig.6).

As per claims 38 Fisher (6,216,229 B1) teach system for securely transmitting data using an unreliable protocol, comprising: a first computer comprising a communication protocol client function operable in conjunction with an application program to transmit data records securely using an unreliable protocol; and a second computer coupled to the first computer and comprising a communication protocol server function operable in conjunction with the communication protocol client function to receive data records securely using the unreliable communication protocol, wherein the communication protocol client function encrypts each data record using a nonce and an encryption key and appends the respective nonce to each of the encrypted data records; and wherein the communication protocol server function decrypts each of the data records using the respectively appended nonce and the encryption key; and a third computer coupled to the second computer and having a cache memory for storing at least the encryption key (as applied to claim 1 above).

As per claim 39 Fisher (6,216,229 B1) teach the system of claim 38, wherein the communication protocol client function exchanges encryption credentials with the communication protocol server function using a reliable communication protocol (see fig.1-6).

As per claim 45 Fisher (6,216,229 B1) teach the system of claim 38, wherein the third computer is a proxy server that can receive encrypted records from the first computer; can decrypt records the received records using at least the encryption key stored in the cache memory; and can forward the decrypted records received from the first computer to a server computer (see fig.6).

Claim Rejections - 35 USC § 103

8. **Claims 5-7, 22-23 and 49-51** are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher (6,216,229 B1) in view of Camp et al (6,317,729 B1).

As per claims 5 and 49 Fisher (6,216,229 B1) teach all limitation of the claim as applied to the method of claim 1, but do not explicitly disclose wherein step (2) of claim 1 comprises the step of incorporating a nonce in each data record that is used by the second computer in combination with a previously shared encryption key to decrypt each of the data records in step (3) of claim 1. However Camp et al. (6,317,729 B1) disclose wherein step (2) comprises the step of incorporating a nonce in each data record that is used by the second computer in combination with a previously shared encryption key to decrypt each of the data records in step (3) (see abstract; col.4, table 1 where a message between the tow party is being described; col.4-5, table 2 where the field in the message that is being transmitted between two party such as computer a and b being describe a nonce, random numbers chall-m and chall-c that corresponds to keys used for encryption or decryption; also see col.7-11). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Camp's nonce and key utilize in SET in Fisher's record in order to offers multiple protocols for electronic commerce which reflect different types of Internet access available.

As per claims 6, 22, 23 and 50 Fisher (6,216,229 B1) teach all limitation of the claim as applied to the method of claims 5 and 20 above, but do not explicitly disclose, wherein the nonce comprises a random number; unique number. However Camp et al. (6,317,729 B1) disclose wherein the nonce comprises a random number (see col.4, table 2, second variable and therefore it is a unique number since it has a random value). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Camp's nonce and key utilize in SET in Fisher's record in order to offers multiple protocols for electronic commerce which reflect different types of Internet access available.

As per claims 7 and 51 Fisher (6,216,229 B1) teach all limitation of the claim as applied to the method of claim 5 above, but do not explicitly disclose, further comprising the step of, in the second computer, verifying that the nonce has not previously been received in a previously transmitted data record. However Camp et al. (6,317,729 B1) disclose , further comprising the step of, in the second computer, verifying that the nonce has not previously been received in a previously transmitted data record (see col.7-11). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Camp's nonce and key utilize in SET in Fisher's record in order to offers multiple protocols for electronic commerce which reflect different types of Internet access available.

9. **Claims 9, 13, 14, 17, 18, 19, 24, 26, 31, 32, 35, 36, 37, 40, 42, 53, 55 and 58** are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher (6,216,229 B1) in view of Applicant Admittance of Prior Art (AAPA).

As per claims 9, 13, 14, 24, 26, 31, 32, 40, 41, 42, 53 and 55 Fisher (6,216,229 B1) teach all limitations of the claim but do not expressly disclose, wherein step (1) is performed using the Transmission Control Protocol, and wherein step (2) is performed using the User Datagram Protocol; wherein the session information is SSL or TLS session information/session identifier; wherein step (1) is performed using Transmission Control Protocol, and wherein step (5) is performed using User Datagram Protocol; wherein the reliable communication protocol is Transmission Control Protocol; are compatible with the SOCKS communication. However AAPA disclose all above limitations on pages 1-8 and page 9, lines 1-20 of the specification as prior art. The motivation for an ordinary skilled in the art to utilize the above limitations in Fisher's method also is disclosed on pages 1-8 and page 9, lines 1-20 of the specification.

As per claims 17 and 35 Fisher (6,216,229 B1) teach all limitations of the claim including the hash function as applied to claims 1 and 20 above but do not expressly disclose, wherein the hash function is the BUZhash function. However AAPA disclose all above limitations on page 29, lines 19-29 and page 30, lines 1-9 of the specification as prior art. The motivation for an ordinary skilled in the art to utilize the above limitations in Fisher's method also is disclosed on pages 30, lines 1-9 of the specification.

As per claims 18, 19, 36, 37 and 58 Fisher (6,216,229 B1) teach all limitation of the claim including transmission of session information between the computers as applied to the method of claims, 1, 11, 12 and 20 but do not expressly disclose using multicast communication; or negative acknowledgment multicast communication. However AAPA disclose all above limitations on page 34, lines 27-29 and page 35, lines 1-15 of the specification as prior art. The motivation for an ordinary skilled in the art to utilize the above limitations in Fisher's method also is disclosed on pages 35, lines 10-13 of the specification.

Allowable Subject Matter

10. **Claims 8, 21, 28, 30, 44 and 46** is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available

through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

12/12/2005

AU 2132